UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA,	:	Criminal No. 11-cr-470 (SDW)
v.	:	**OPINION**
ANDREW AUERNHEIMER,	:	October 26, 2012
Defendant.	:	

WIGENTON, District Judge.

Before the Court is Defendant Andrew Auernheimer's ("Defendant" or Auernheimer") Motion to Dismiss the Superseding Indictment ("Motion"). The United States of America ("Government") opposed the Motion. For the reasons stated below, the Court DENIES Defendant's Motion.

FACTUAL AND PROCEDURAL HISTORY

Although the Court assumes the parties' familiarity with the allegations and procedural history in the case, the Court will briefly review the facts relevant to the present Motion. In June 2010, Defendant and former co-defendant, Daniel Spitler ("Spitler"), created a computer program, the "Account Slurper" ("Program"), designed to exploit AT&T's automated feature which linked iPad 3G users' e-mail addresses to their unique iPad 3G Integrated Circuit Card Identifiers ("ICC-ID"). (Superseding Indictment, Count 1, ¶¶ 7-8.) Specifically, the Program "was designed to mimic the behavior of an iPad 3G so that AT&T's servers were fooled into believing that they were communicating with an actual iPad 3G and wrongly granted the [Program] access to AT&T's servers." (Id. at Count 1, ¶ 8a.) Between June 5, 2010 and June 9, 2010, Defendant and Spitler's Program gained unauthorized access to AT&T's servers and obtained approximately 120,000 ICC-ID/e-mail address pairings from iPad 3G customers, including thousands of customers in New Jersey. (Id. at Count 1, ¶¶ 9, 27d.) Subsequently, Defendant and Spitler disclosed the stolen ICC-ID/e-mail address pairings to Gawker, an Internet magazine, and sent e-mails to members of various news organizations offering "to describe the method of theft in more detail." (Id. at Count 1, ¶¶ 11, 12, 24 & n.4, 27c.)

On August 16, 2012, a federal grand jury sitting in Newark, New Jersey returned a two-count Superseding Indictment against Defendant. Count One charged that, from June 2, 2010 through June 15, 2010, Defendant conspired to access a computer without authorization or exceeded authorized access, and thereby obtained information from a protected computer, in furtherance of a criminal act in violation of N.J.S.A. 2C:20-31(a), contrary to the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(B)(ii), in violation of 18 U.S.C. § 371. Count Two charged that, from June 2, 2010 through June 15, 2010, Defendant knowingly transferred, possessed, and used, without lawful authority, means of identification of other persons, including New Jersey residents, in connection with unlawful activity, specifically, the unlawful accessing of AT&T's servers contrary to 18 U.S.C. § 1030(a)(2)(C), in violation of 18 U.S.C. §§ 1028(a)(7) and section 2.

LEGAL STANDARD

An indictment, if valid on its face and returned by a legally constituted and unbiased grand jury, "is enough to call for trial of the charge on the merits." United States v. Vitillo, 490 F.3d 314, 320 (3d Cir. 2007) (quoting Costello v. United States, 350 U.S. 359, 363 (1956)). "An indictment is generally deemed sufficient if it: [ ] (1) contains the elements of the offense intended to be charged, (2) sufficiently apprises the defendant of what he must be prepared to meet, and (3) allows the defendant to show with accuracy to what extent he may plead a former acquittal or conviction in the event of a subsequent prosecution." Id. (quoting United States v. Rankin, 870 F.2d 109, 112 (3d Cir. 1989)) (internal quotation marks omitted).

"Federal Rule of Criminal Procedure 12(b)(3)(B) allows a district court to review the sufficiency of the government's pleadings to . . . ensure that legally deficient charges do not go to a jury." United States v. Huet, 665 F.3d 588, 595 (3d Cir. 2012) cert. denied, No. 11-10312, 2012 WL 1716258 (Oct. 9, 2012) (quoting United States v. Bergrin, 650 F.3d 257, 268 (3d Cir. 2011)) (internal quotation marks omitted); see United States v. DeLaurentis, 230 F.3d 659, 661 (3d Cir. 2000) ("Federal Rule of Criminal Procedure [12(b)(3)(B)] authorizes dismissal of an indictment if its allegations do not suffice to charge an offense.") Although the Government is not obligated to bring forward its entire case in the indictment, "if the specific facts" alleged "fall beyond the scope of the relevant criminal statute, as a matter of statutory interpretation," then the indictment fails to state an offense. Huet, 665 F.3d at 595 (quoting United States v. Panarella, 277 F.3d 678, 685 (3d Cir. 2002)). "Evidentiary questions—such as credibility determinations and the weighing of proof—should not be determined at this stage." Bergrin, 650 F.3d at 265 (quoting United States v. Gallagher, 602 F.2d 1139, 1142 (3d Cir. 1979)) (internal quotation marks omitted). Accordingly, "a district court's review of the facts set forth in the indictment is limited to determining whether, assuming all of those facts as true, a jury could find that the defendant committed the offense for which he was charged." Huet, 665 F.3d at 595-96.

DISCUSSION

Defendant moves to dismiss the Superseding Indictment based on five arguments: (1) the CFAA is void for vagueness; (2) Count One poses a merger problem resulting in double jeopardy; (3) the District of New Jersey is not a proper venue for this action; (4) Count Two is improperly pled because under 18 U.S.C. § 1028(a)(7), the offense cannot be "in connection with" a past crime; and (5) Count Two violates the First Amendment. For the reasons stated below, Defendant's Motion is denied. Each argument is addressed in detail below.

I. Count One: CFAA is Void for Vagueness Under the Fifth Amendment's Due Process Clause

A CFAA offense pursuant to 18 U.S.C. § 1030(a)(2)(C) occurs when an individual "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer[.]" Defendant argues that the CFAA is unconstitutionally vague as applied because it does not provide notice that the charged conduct was illegal. Specifically, Defendant contends that "[t]he CFAA provides no definition as to what constitutes unauthorized access to a protected computer, and the courts are conflicted as to what unauthorized access means." (Def. Br. 4.)

Although Defendant is correct that the statute does not define "without authorization," following a well-established canon of statutory construction, several courts have construed this phrase based on its ordinary, dictionary definition. See Perrin v. United States, 444 U.S. 37, 42 (1979). For instance, in WEC Carolina Energy Solutions LLC v. Miller, the Fourth Circuit concluded that in the context of a CFAA violation, "based on the 'ordinary, contemporary, common meaning,' of 'authorization,'. . . [an individual] accesses a computer 'without authorization' when he gains admission to a computer without approval." 687 F.3d 199, 204 (4th Cir. 2012) (citations omitted). Similarly, the Sixth Circuit stated in Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am. that because "Congress left the interpretation of 'without authorization' to the courts, we again start with ordinary usage. The plain meaning of 'authorization' is '[t]he conferment of legality; . . . sanction.' Commonly understood, then, a defendant who accesses a computer 'without authorization' does so without sanction or permission." 648 F.3d 295, 303-04 (6th Cir. 2011) (citing 1 Oxford English Dictionary 798 (2d ed. 1989)). Lastly, in examining the CFAA statute in LVRC Holdings LLC v. Brekka, the Ninth Circuit applied "the "ordinary, contemporary, common meaning" of "without authorization." 581 F.3d 1127, 1133 (9th Cir. 2009) (concluding that based on the plain meaning of the terms, individual did not act "without authorization").

Additionally, "[i]t is well established that vagueness challenges to statutes which do not involve First Amendment freedoms must be examined in light of the facts of the case at hand." United States v. Moyer, 674 F.3d 192, 211 (3d Cir. 2012) (quoting United States v. Mazurie, 419 U.S. 544, 550 (1975)). "In criminal cases, because vagueness attacks are based on lack of notice, they may be overcome in any specific case where reasonable persons would know their conduct puts [them] at risk of punishment under the statute." Id. (internal quotation and citation omitted) (alteration in original). Defendant's vagueness challenge involves the CFAA and not First Amendment freedoms; thus, the Court will conduct its analysis "in light of the facts of the case at hand." See id.

Based on the circumstances in this case, this Court is satisfied that the CFAA is not unconstitutionally vague and that "reasonable persons would know their conduct puts [them] at risk of punishment under the statute." See Moyer, 647 F.3d at 211. The Superseding Indictment specifically alleges that Defendant gained unauthorized access to AT&T servers, stole 120,000 ICC-ID email address pairings, and committed the theft without authorization. (Superseding Indictment, Count 1, ¶¶ 9-10, 27d.) In his own words, Defendant even offered to provide the press with details of his "method of theft." (Id. at Count 1, ¶ 24.) The Superseding Indictment sufficiently alleges the elements of unauthorized access and sufficiently alleges conduct demonstrating Defendant's knowledge and intent to gain unauthorized access. For the purpose of Defendant's Motion, accepting the allegations in the Superseding Indictment as true and in light of the facts at hand, the Court finds that the CFAA is not vague. Thus, Defendant's Motion fails with respect to this argument.[1]

II. Count One: Double Jeopardy Under the Fifth Amendment

Under the Fifth Amendment's Double Jeopardy Clause, a defendant may not be charged or punished twice for the same offense. U.S. Const. Amend. V ("nor shall any person be subject for the same offense be twice put in jeopardy of life or limb"). A "merger problem tantamount to double jeopardy" occurs "where the facts or transactions alleged to support one offense are also the same used to support another." United States v. Cioni, 649 F.3d 276, 282 (4th Cir. 2011) (internal citations and quotations omitted). For example, in Cioni, the Fourth Circuit found that a merger problem arose where "the indictment [did] not allege facts sufficient to indicate that [ ] two crimes were based on distinct conduct" and instead were "actually based on [defendant's] single unsuccessful attempt to access [an] electronic e-mail account." Id. at 283. The Fourth Circuit clarified that "[i]f the government had proven that [defendant] accessed [the] e-mail inbox and then used the information from that inbox to access another person's electronic communications, no merger problem would have arisen."[2] Id.

[1] The Court notes that Defendant requested application of the Rule of Lenity to "narrow the CFAA to mean bypassing code based restrictions such as passwords or firewalls." (Def. Br. 7.) The cases cited by Defendant do not lend support to his argument that CFAA violations must always be read to require the bypassing of computer security measures. See Cvent, Inc. v. Eventbrite, Inc., 739 F. Supp. 2d 927, 933 (E.D. Va. 2010); Koch Indus., v. Does, 10-cv-1275, 2011 WL 1775765, at *8 (D. Utah May 9, 2011). Additionally, in finding that the CFAA is not constitutionally vague in this case and poses no threat of Defendant's concern that "the government [ ] pursue expansive interpretations against unpopular defendants and then wield its expansive interpretation arbitrarily," the Court declines to apply the Rule of Lenity. (Def. Br. 7.)

[2] In Cioni, the Fourth Circuit additionally concluded that a merger problem arose where the Government relied on the same conduct to support an underlying statutory violation as well as the elevating violation. 649 F.3d at 282. Although the two crimes were "distinct and different," the Government's failure to articulate additional evidence in support of the elevating violation posed a merger problem. Id. at 283. Importantly, in Cioni, the Government conceded the merger problem, recognizing that "there was no evidence that the defendant committed this offense 'in furtherance of any' separate and distinct'" elevating violation. Id. at 282 (citations omitted).

Count One of the Superseding Indictment charges Defendant with conspiracy to access a computer without authorization or to exceed authorized access, and thereby obtain information from AT&T's servers (in violation of the CFAA, punishable as a felony), in furtherance of a New Jersey criminal statute, N.J.S.A. 2C:20-31(a). Defendant argues that "Count One violates the Double Jeopardy Clause because it improperly aggravates a CFAA misdemeanor into a felony." (Def. Br. 8.) Specifically, Defendant asserts that the object of the conspiracy—the CFAA offense—relies on proof of the same facts and conduct as the felony aggravator—N.J.S.A. 2C:20-31(a). (Def. Br. 8-9.)

As the Government correctly points out, the CFAA and N.J.S.A. 2C:20-31(a) do not require the same proof of conduct. (See Gov't Br. 23.) Moreover, in this case, the Government does not rely on the same allegations for the two offenses in the Superseding Indictment.

The CFAA requires two elements to establish a violation: (1) defendant "intentionally accesses a computer without authorization or exceeds authorized access" and (2) defendant "thereby obtains . . . information from any protected computer." 18 U.S.C. § 1030(2)(A). A CFAA violation is generally a misdemeanor; however, it is punishable as a felony if the offense is "committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C. § 1030(c)(2)(B)(ii).[3]

An offense under N.J.S.A. 2C:20-31(a) requires three elements to establish a violation: (1) defendant purposely or knowingly accessed data; (2) defendant accessed the data "without authorization, or in excess of authorization;" and (3) defendant "knowingly or recklessly discloses or causes to be disclosed any data . . . or personal identifying information." N.J.S.A. 2C:20-31(a).

[3] In this case, the Superseding Indictment alleges that the CFAA violation was in furtherance of a New Jersey felony criminal statute, N.J.S.A. 2C:20-31(a); thus, the offense is elevated to a felony. (Superseding Indictment, Count 1, ¶¶ 5, 27.)

Although there is an overlap of facts for the first two elements of each offense, N.J.S.A. 2C:20-31(a) requires the additional component that defendant "knowingly or recklessly discloses or causes to be disclosed any data . . . or personal identifying information." Hence, an essential N.J.S.A. 2C:20-31(a) element requires proof of conduct not required for a CFAA offense. The Government specifically alleges in the Superseding Indictment that defendant and his co-conspirators "knowingly disclosed approximately 120,000 stolen ICC-ID/email address pairings for iPad 3G customers . . . to the internet magazine Gawker." (Superseding Indictment, Count 1, ¶ 27d.) Accordingly, Defendant's Motion is denied with respect to this argument.

III. Venue in the District of New Jersey For Both Counts of the Superseding Indictment

Defendant contends that this Court lacks jurisdiction over Counts One and Two. In support of his argument, Defendant argues that "no alleged fact which, if ultimately proven, took place in New Jersey." (Def. Br. 13.)

Count One

In the absence of an express venue provision in a criminal statute, courts determine venue based on the "nature of the crime alleged and the location of the act or acts constituting it." United States v. Rodriguez-Moreno, 526 U.S. 275, 279 (1999) (internal quotations and citations omitted). Pursuant to 18 U.S.C. § 3237, "any offense against the United States begun in one district and completed in another, or committed in more than one district, may be inquired of and prosecuted in any district in which such offense was begun, continued, or completed." For instance, in United States v. Powers, in the context of an alleged violation of the CFAA, "[a]lthough [defendant] may not have been physically present in Nebraska, and the computer used to facilitate the violation was located in Arizona," venue was proper in the District of Nebraska because defendant's CFAA violation injured a Nebraska resident and violated

Nebraska tort laws. No. 09-361, 2010 WL 1418172, at *2 (D. Neb. Mar. 4, 2010) (noting that "[v]enue would not only be proper in the District of Arizona where the crime began, but also in the District of Nebraska where the crime was completed").

The reasoning in Powers is instructive in this case with respect to Count One. Although Defendant was not present in New Jersey and did not gain access to a computer in New Jersey, his alleged CFAA violation, in furtherance of the alleged conspiracy, was completed in New Jersey. Defendant's purported conduct—knowing disclosure of personal identifying information to the press—affected thousands of New Jersey residents and violated New Jersey law. Similar to the reasoning in Powers, because a defendant can be prosecuted in any district where the crime began, continued, or completed, this Court finds that venue is proper in the District of New Jersey regarding Count One.

Count Two

"Where . . . a defendant is charged with multiple crimes in a single indictment, the government must satisfy venue with respect to each charge." United States v. Davis, 689 F.3d 179, 185 (2d Cir. 2012). As the Third Circuit has noted, "[t]he locality of a crime for the purpose of venue extends 'over the whole area through which force propelled by an offender operates.'" United States v. Root, 585 F.3d 145, 156 (3d Cir. 2009) (citing United States v. Johnson, 323 U.S. 273, (1944)).

Section 1028(a)(7) disallows certain conduct "in connection with, any unlawful activity that constitutes a violation of Federal law[.]" Thus, the predicate federal offense is an essential element to a § 1028(a)(7) charge. Accordingly, venue for § 1028(a)(7) violations is likely proper in any district in which venue is proper for the predicate violation of federal law. See e.g., United States v. Magassouba, 619 F.3d 202, 206 (2d Cir. 2010) (holding that "venue properly lies with respect to an aggravated identity theft offense in any district in which venue lies for the predicate"). The predicate federal offense in this case is Defendant's alleged CFAA violation. As the CFAA violation is a key factor to the § 1028(a)(7) charge, venue lies in any district where the crime began, continued, or completed. See 18 U.S.C. § 3237(a). Because there is venue in the District of New Jersey for the predicate federal offense—the CFAA violation which is the object of Count One's conspiracy charge—this Court finds that venue is also proper for Count Two.[4]

IV. Count Two: Improper Violation Under 18 U.S.C. § 1028(a)(7)

The criminal statute at issue in Count Two, 18 U.S.C. § 1028(a)(7), states in pertinent part:

> "[w]hoever . . . transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law . . . shall be punished as provided in subsection (b) of this section."

18 U.S.C. § 1028(a)(7). According to Defendant, the statute requires alleged violations to be "in connection with" a present or future criminal activity and not a past criminal act. (See Def. Br. 16.) Based on this interpretation, Defendant argues that Count Two improperly pleads a § 1028(a)(7) violation because Defendant's alleged transfer, possession, and use of others' identification commenced after the CFAA violation was complete. (See Def. Br. 16.)

Defendant's interpretation of § 1028(a)(7) is contrary to the statute's legislative history and is unsupported by case law. As the Government points out, Congress amended the statute in

[4] Although unnecessary to address, the Court acknowledges the Government's additional venue arguments. The Government argues that venue is proper on both Counts as they charge "continuing" offenses under 18 U.S.C. § 3237(a). (Gov't Br. 33.) Moreover, according to the Government, "[w]here an offense requires the United States to prove the failure to do or obtain something, that offense may be prosecuted in the district where the failure occurs." (Gov't Br. 34.) The Government contends that venue is proper on both Counts as the Government must prove that defendant accessed AT&T's computers "without authorization" from AT&T or its customers, the victims in New Jersey. (Gov't Br. 34.)

2004 to include the words "in connection with" to "broaden the reach of section 1028(a)(7)." H.R. Rep. No. 108-528, at 10 (2004), available at 2004 WL 1260964, at *10 (stating that the phrase "in connection with" would serve to "make possible the prosecution of persons who knowingly facilitate the operations of an identity-theft ring . . . but who may deny that they had the specific intent to engage in a particular fraud scheme[, and] it will provide greater flexibility for the prosecution of section 1028(a)(7) offenses"). Neither the face of the statute nor legislative history indicates that the statutory phrase "in connection with" necessitates a temporal restriction for § 1028(a)(7) violations.

Additionally, the two cases to which Defendant cites do not lend support for his argument that the phrase "in connection with" requires an allegation of a present or future crime and not a past crime. See U.S. v. Sutcliffe, 505 F.3d 944, 959 (9th Cir. 2007) (analyzing § 1028(a)(7) violation pursuant to pre-2004 Amendment language which did not include the phrase "in connection with"); U.S. v. Villanueva-Sotelo, 515 F.3d 1234, 1245-46 (D.C. Cir. 2008) (referencing the amended § 1028(a)(7) in passing, but not indicating that Congress intended only to prosecute those engaging in present or future crimes). However, even using Defendant's interpretation of the statute, the Superseding Indictment alleges that at least part of Defendant's unauthorized computer access overlapped with his possession and transfer of persons' identification, from June 2, 2010 through June 15, 2010. (Superseding Indictment, Count 1, ¶ 5; Count 2, ¶ 2.) Accordingly, the Court finds that the Superseding Indictment sufficiently and properly pleads a § 1028(a)(7) violation; thus Defendant's Motion fails with respect to this argument.

V. Count Two: Violation of the First Amendment

Defendant argues that Count Two violates the First Amendment because it criminalizes Defendant's "transmission of publicly available information on matters of important public concern to the press." (Def. Br. 18.) In further support of his argument, Defendant contends that he "served the public by exposing AT&T's non-existent security and cavalier disregard of its customers' information." (Def. Br. 18.)

As specifically noted in the Superseding Indictment, "[t]he ICC-IDs and iPad user e-mail addresses were not available to the public and were kept confidential by AT&T." (Superseding Indictment, Count 1, ¶ 1o; see Count 2, ¶ 1 (incorporating ¶¶ 1-4; 7-27).) The very conduct at issue involves Defendant's allegedly unauthorized access to a protected computer and the subsequent transfer of such confidential information. Additionally, as the Supreme Court has held, "[i]t rarely has been suggested that the constitutional freedom for speech and press extends its immunity to speech or writing used as an integral part of conduct in violation of a valid criminal statute." New York v. Ferber, 458 U.S. 747, 761-62 (1982) (internal citations and quotations omitted). Accordingly, Defendant's Motion fails with respect to this argument.

CONCLUSION

For the reasons stated above, this Court DENIES Defendant's Motion.

s/Susan D. Wigenton, U.S.D.J.